CLOUD.GOV

Peter Burkholder

You and your platform

- Mission / Concept
- Team / Skills
  - UX, Engineers, DataSci, ...
- Platform:
  - Build
  - Test
  - Run
- How to procure, build, secure, maintain?

Iván García, MX, 2013 World Diving Championships, Barcelona - Rob Nunn

Platform

- **Stack**: WebServer, AppServer, Database, Cache, Index
- **Environments**: (Local), Dev, Test, Stage, Prod
- **User management**: Admin, Devs, Auditors
- **Operations**: Patch, Logs, CDN, Scanning, Availability

All of this is commodity

Acquire: weeks // **Running**: hours // **Build**: months // **Authorize**: weeks

Platform as a Service

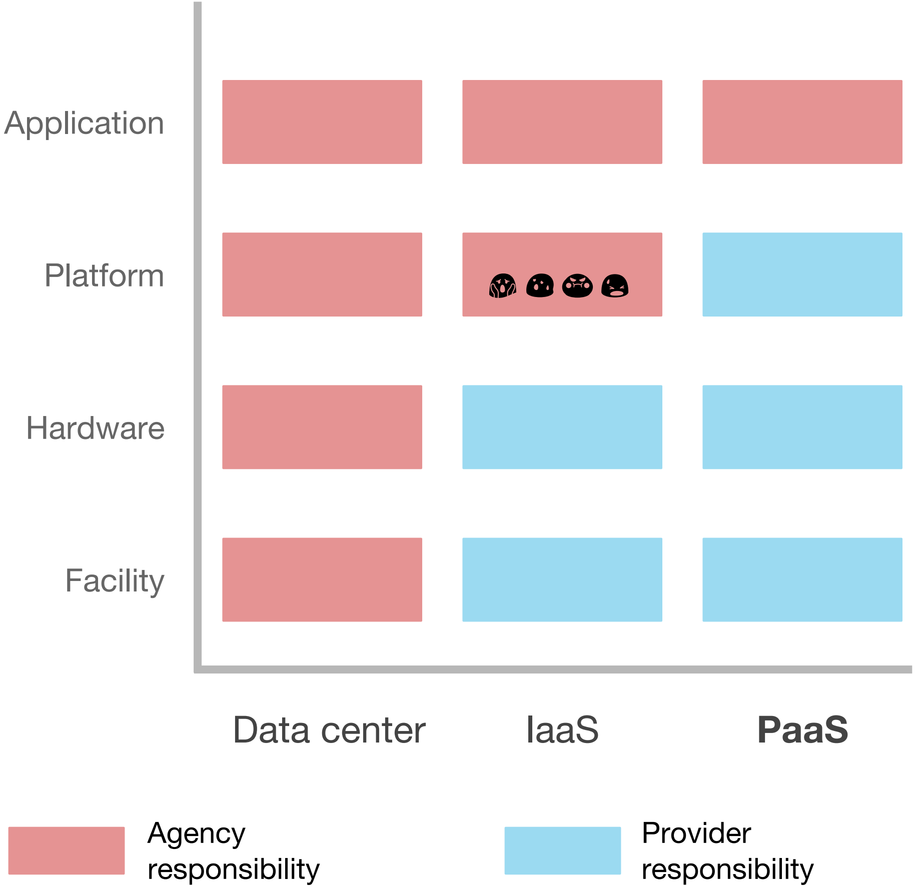
Pre-built environment ready for deploying an application

Developers can focus on mission needs

Common technology resources are managed by an expert operations team

- Operating system
- Databases
- Audit trails
- Authentication
- Authorization
- Load balancing
- Scaling
- Vulnerability scans
- Programming languages
- Automated updates

Reduce what you manage that's common across the government.



	Data center	IaaS	**PaaS**
Application	🟥	🟥	🟥
Platform	🟥	🟥	🟦
Hardware	🟥	🟦	🟦
Facility	🟥	🟦	🟦

🟥 Agency responsibility

🟦 Provider responsibility

How we do this

cloud.gov is a **Platform as a Service** (PaaS).

It is based on **open source** Cloud Foundry and built on AWS GovCloud.

It has baked-in **federal security compliance.**

CLOUD.GOV

CLOUD FOUNDRY

AWS GovCloud (US)

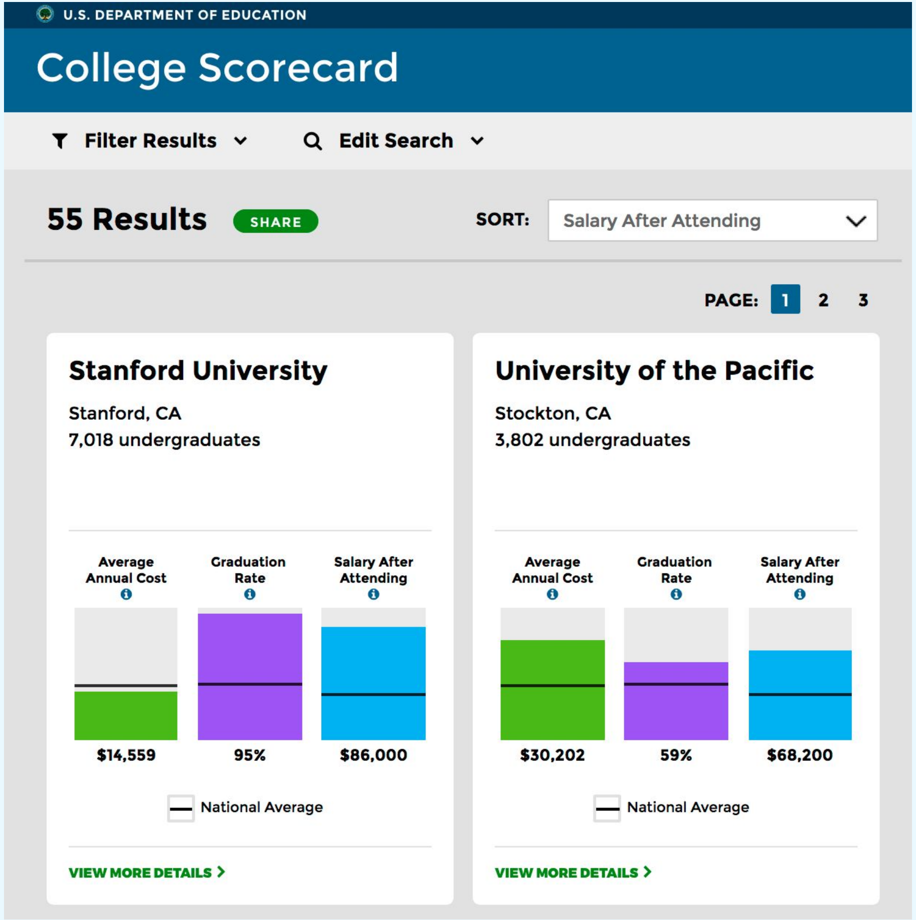
amazon
web services

How it works

Your team brings **custom or COTS software**.

They use **self-service tools to configure services** for databases, storage, CDN, etc.

They **deploy** the application.



U.S. DEPARTMENT OF EDUCATION

College Scorecard

55 Results

SORT: Salary After Attending

PAGE: 1 2 3

Stanford University

Stanford, CA
7,018 undergraduates

Average Annual Cost	Graduation Rate	Salary After Attending
$14,559	95%	$86,000

— National Average

VIEW MORE DETAILS ›

University of the Pacific

Stockton, CA
3,802 undergraduates

Average Annual Cost	Graduation Rate	Salary After Attending
$30,202	59%	$68,200

— National Average

VIEW MORE DETAILS ›

Self-service

Create an environment:

```
cf create-space staging
```

Create a database:

```
cf create-service aws-rds medium-oracle-se2 forest-data
```

Deploy your application:

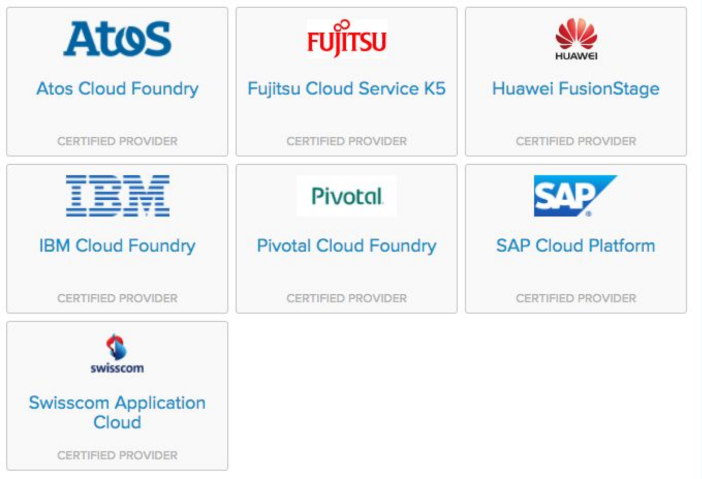
```
cf push tree-app
```

Scale your application:

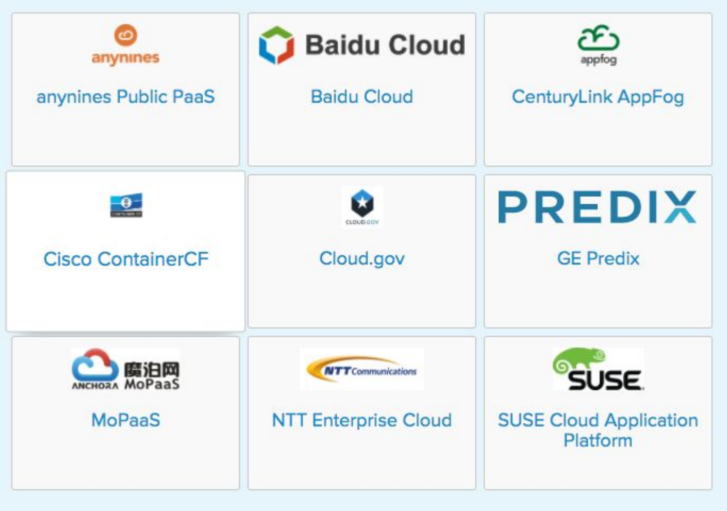
```
cf scale tree-app -i 2
```

Cloud Foundry

- **Actively developed and updated**
  - Open source Platform as Service with many active contributors
- **Large community**
  - Thriving ecosystem with 400+ system integrators and consultants
- **Reduces vendor lock-in**
  - Multiple industry installations
  - Code supports multiple IaaS providers



Atos Cloud Foundry CERTIFIED PROVIDER	Fujitsu Cloud Service K5 CERTIFIED PROVIDER	Huawei FusionStage CERTIFIED PROVIDER
IBM Cloud Foundry CERTIFIED PROVIDER	Pivotal Cloud Foundry CERTIFIED PROVIDER	SAP Cloud Platform CERTIFIED PROVIDER
Swisscom Application Cloud CERTIFIED PROVIDER		



anynines Public PaaS	Baidu Cloud	CenturyLink AppFog
Cisco ContainerCF	Cloud.gov	GE Predix
MoPaaS	NTT Enterprise Cloud	SUSE Cloud Application Platform

Reducing vendor lock-in

Applications that work with cloud.gov **also work with industry Cloud Foundry providers.**

Expanding vendor choice

Third-party contractors can bid on how they build software, as most of the **operational concerns** have been offloaded.

Authorizations

FedRAMP JAB P-ATO Moderate

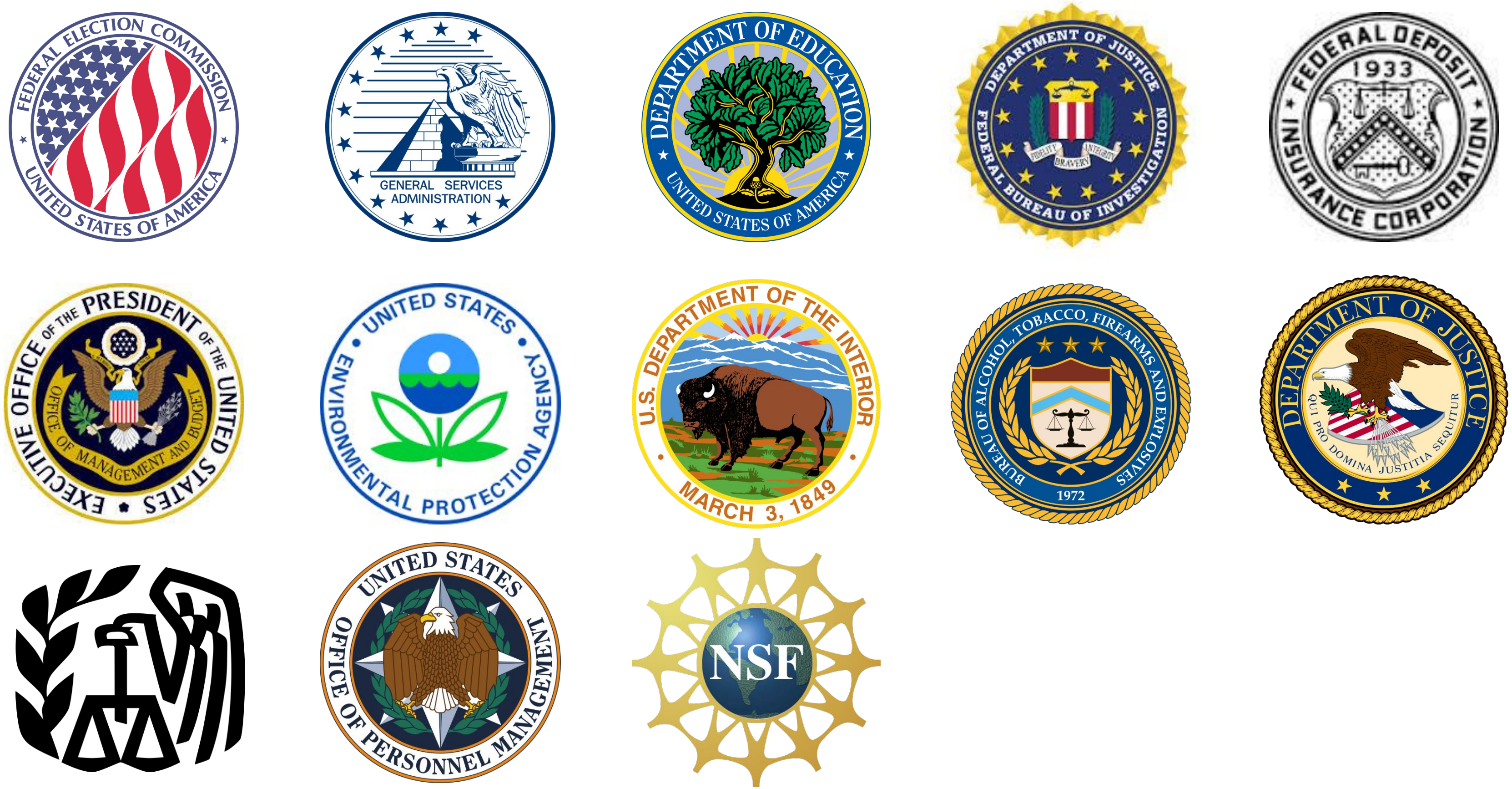
DISA DoD P-ATO Impact Level 2

You review authorizations, but **only assess your own application.**

FedRAMP

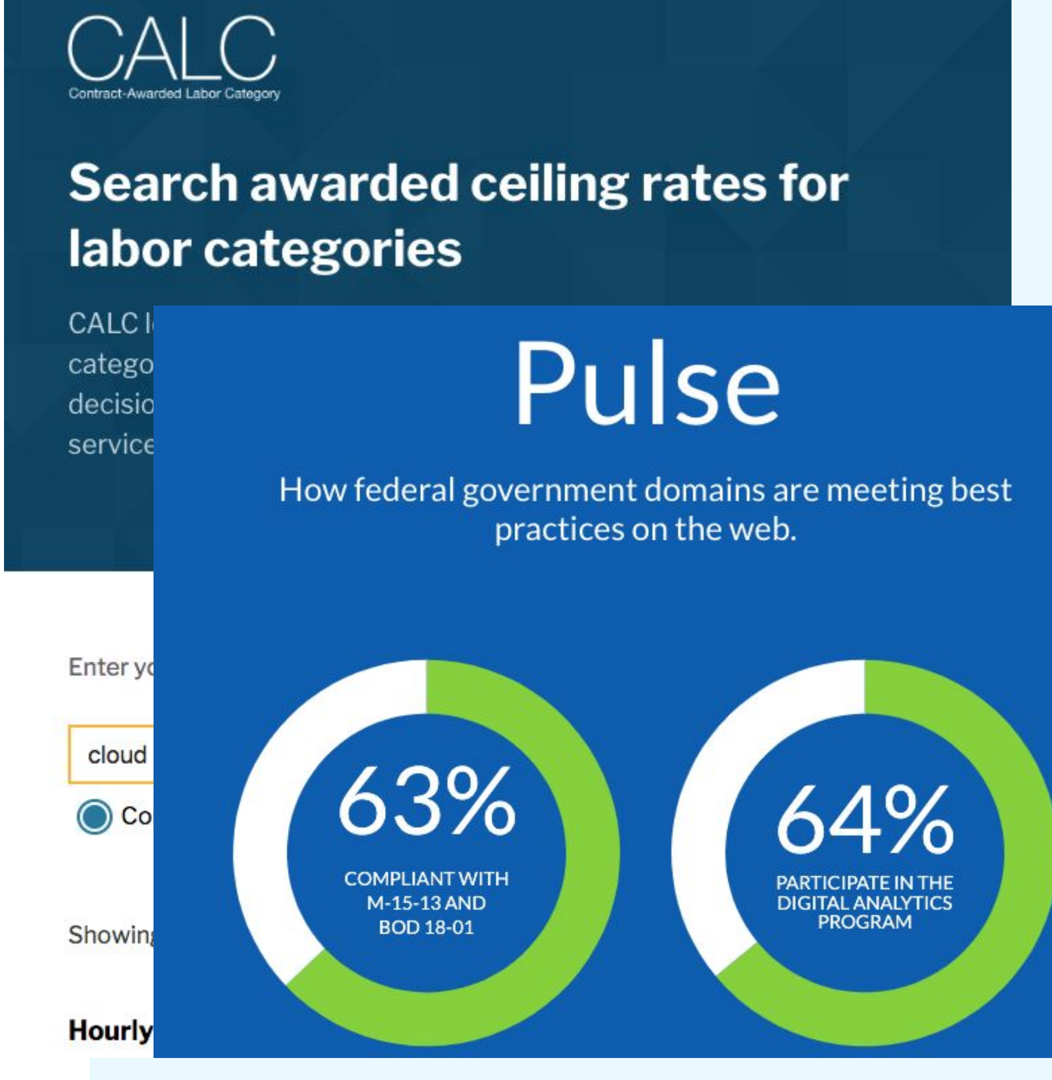
DISA

Current customers


FEDERAL ELECTION COMMISSION
UNITED STATES OF AMERICA
GENERAL SERVICES ADMINISTRATION
DEPARTMENT OF EDUCATION
UNITED STATES OF AMERICA
DEPARTMENT OF JUSTICE
FIDELITY BRAVERY INTEGRITY
FEDERAL BUREAU OF INVESTIGATION
FEDERAL DEPOSIT
1933
INSURANCE CORPORATION
EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
OFFICE OF MANAGEMENT AND BUDGET
UNITED STATES
ENVIRONMENTAL PROTECTION AGENCY
U.S. DEPARTMENT OF THE INTERIOR
MARCH 3, 1849
BUREAU OF ALCOHOL, TOBACCO, FIREARMS AND EXPLOSIVES
1972
DEPARTMENT OF JUSTICE
QUI PRO DOMINA JUSTITIA SEQUITUR
UNITED STATES
OFFICE OF PERSONNEL MANAGEMENT
NSF

GSA sampling

- FAS: calc.gsa.gov
- OGP: pulse.cio.gov
- OPP: analytics.usa.gov
- TTS: Federalist
- FEDSIM Express (pre-production)
- Two more at OGP (pre-production)
- CTO office (prototyping)



CALC

Contract-Awarded Labor Category

Search awarded ceiling rates for labor categories

CALC l

catego

decisio

service

Enter yo

cloud

○ Co

Showin

Hourly

Pulse

How federal government domains are meeting best practices on the web.

63%
COMPLIANT WITH M-15-13 AND BOD 18-01
64%
PARTICIPATE IN THE DIGITAL ANALYTICS PROGRAM

Where to?

- Technical Demo
- Case Studies
- Running on cloud.gov
  - E.g languages, services
- Compliance
- Packages
  - prototyping/Fisma low, etc

CLOUD.GOV

Demo: launch a Java app, attach DB

Case Studies

CLOUD.GOV

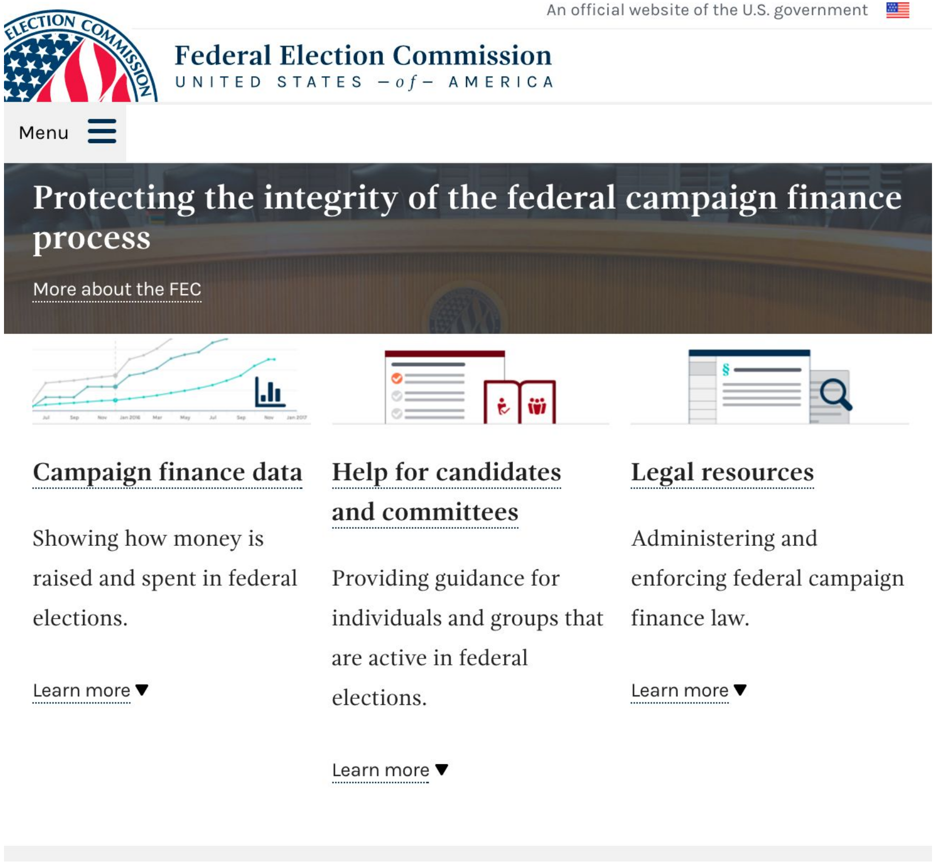
GSA

18F

Federal Election Commission (fec.gov)

FEC spent $1.4 million annually on their data center

With cloud.gov + AWS, initial estimates show **$1.2 million in savings annually**



An official website of the U.S. government

Federal Election Commission
UNITED STATES –of– AMERICA

Menu

Protecting the integrity of the federal campaign finance process

More about the FEC

Campaign finance data

Showing how money is raised and spent in federal elections.

Learn more ▼

Help for candidates and committees

Providing guidance for individuals and groups that are active in federal elections.

Learn more ▼

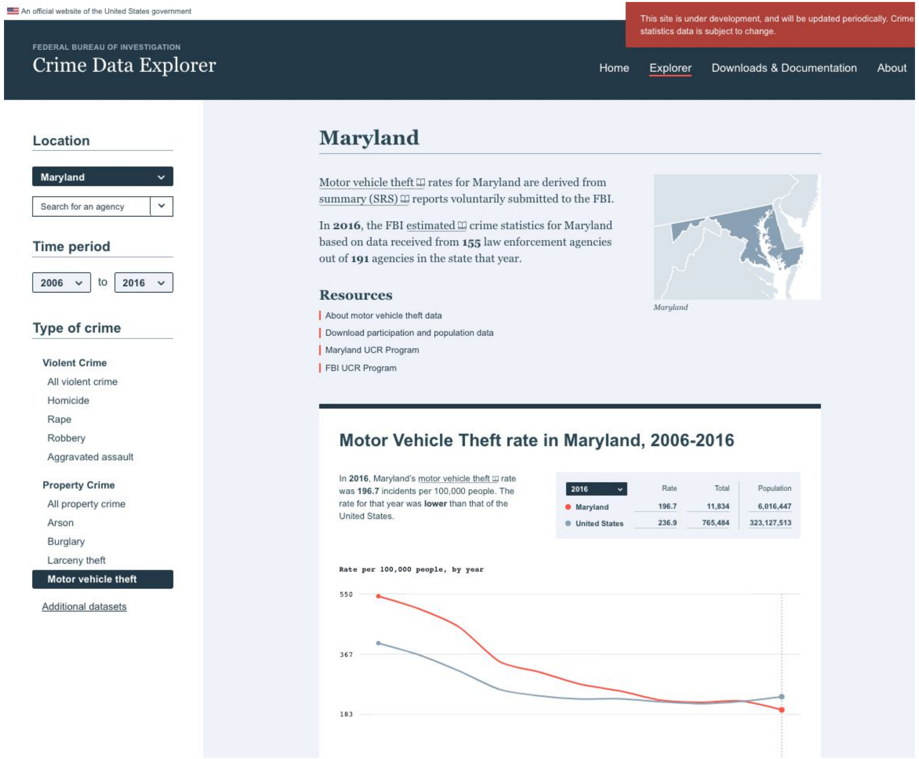
Legal resources

Administering and enforcing federal campaign finance law.

Learn more ▼

Prototyping packages

- FDIC
  - Adopting Agile/DevOps more broadly
- FBI Crime Data Explorer
  - FBI Crime Data Explorer visualizes crime trends, offers bulk datasets, and an open API. Python web app with ~1Tb RDS PostgreSQL databases.
- NOAA



An official website of the United States government

This site is under development, and will be updated periodically. Crime statistics data is subject to change.

FEDERAL BUREAU OF INVESTIGATION

Crime Data Explorer

Maryland

Motor vehicle theft rates for Maryland are derived from summary (SRS) reports voluntarily submitted to the FBI.

In **2016**, the FBI estimated crime statistics for Maryland based on data received from **155** law enforcement agencies out of **191** agencies in the state that year.

Resources

- About motor vehicle theft data
- Download participation and population data
- Maryland UCR Program
- FBI UCR Program

Motor Vehicle Theft rate in Maryland, 2006-2016

In **2016**, Maryland's motor vehicle theft rate was **196.7** incidents per 100,000 people. The rate for that year was **lower** than that of the United States.

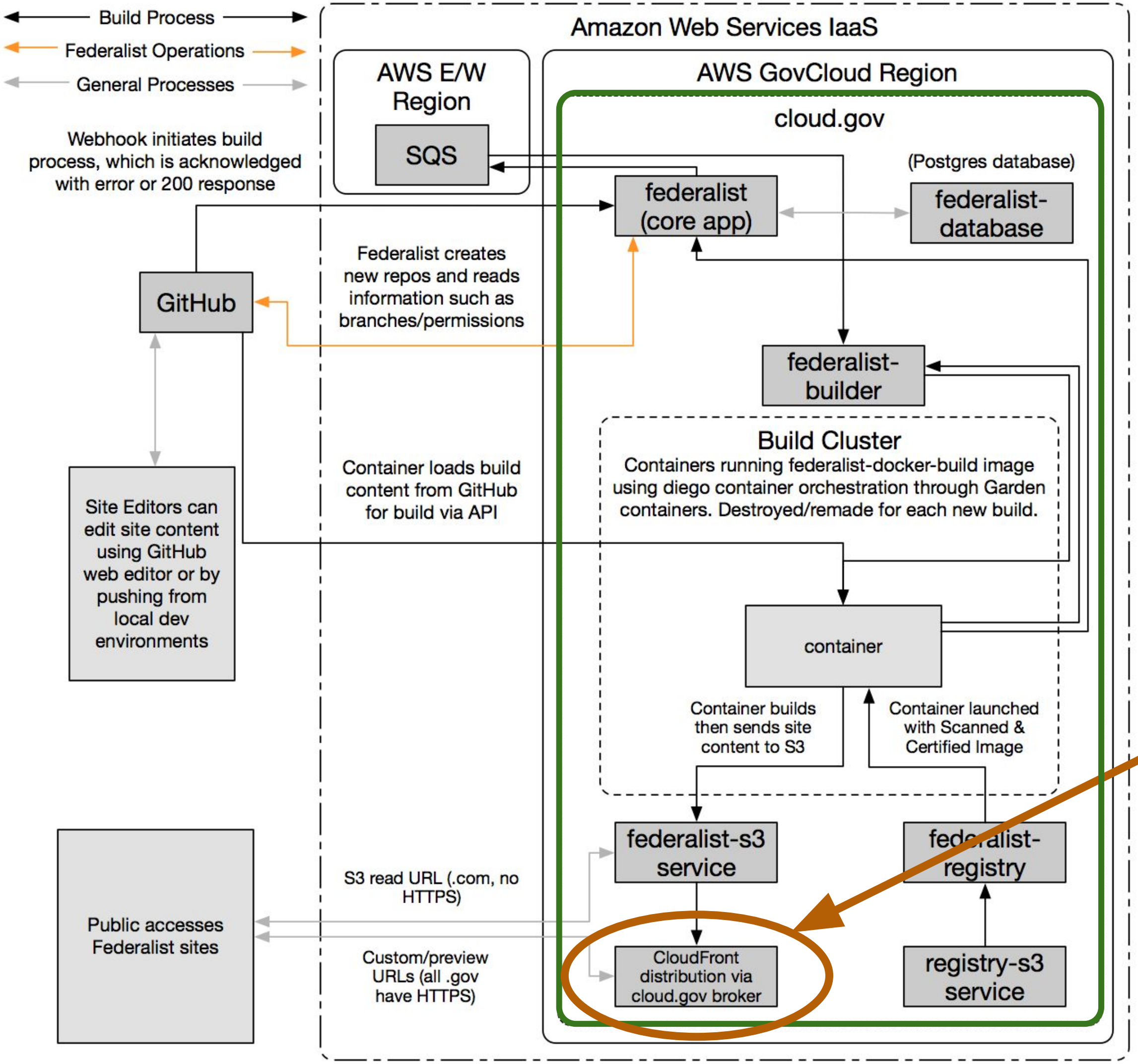
2016	Rate	Total	Population
● Maryland	196.7	11,834	6,016,447
● United States	236.9	765,484	323,127,513

Rate per 100,000 people, by year

Federalist

- Running a static website in the government to inform the public can be extraordinarily difficult
- Federalist
  - makes it easy for teams to publish/update
  - enables feds to focus on content
- Examples:
  - DOI Revenue Data
  - Plainlanguage.gov
  - FedRAMP
  - 116 others ...

https://federalist.18f.gov/


Build Process
Federalist Operations
General Processes
Webhook initiates build process, which is acknowledged with error or 200 response
Amazon Web Services IaaS
AWS E/W Region
SQS
AWS GovCloud Region
cloud.gov
federalist (core app)
(Postgres database)
federalist-database
GitHub
Federalist creates new repos and reads information such as branches/permissions
federalist-builder
Build Cluster
Containers running federalist-docker-build image using diego container orchestration through Garden containers. Destroyed/remade for each new build.
Site Editors can edit site content using GitHub web editor or by pushing from local dev environments
Container loads build content from GitHub for build via API
container
Container builds then sends site content to S3
Container launched with Scanned & Certified Image
federalist-s3 service
federalist-registry
Public accesses Federalist sites
S3 read URL (.com, no HTTPS)
Custom/preview URLs (all .gov have HTTPS)
CloudFront distribution via cloud.gov broker
registry-s3 service

Federalist leverages these cloud.gov managed tools:

- Webapp
- Some utility apps
- RDS database
- Proxy app
- A set of worker containers
- Two s3 services
- Many, many CDN services

One admin command required to launch a new site on Federalist:

```
cf
create-service
cdn-route
```

Customer then CNAME's DNS to the cloud.gov-brokered cloudfront route and HTTPS is automatically set up by the CDN broker

Running on cloud.gov

CLOUD.GOV

Well-suited for cloud.gov

- ❑ **Modern web applications.** Built in the last 5-7 years
- ❑ **Linux.** Runs on a *nix operating system

.Net Core Java Go

Ruby Node.js Python PHP

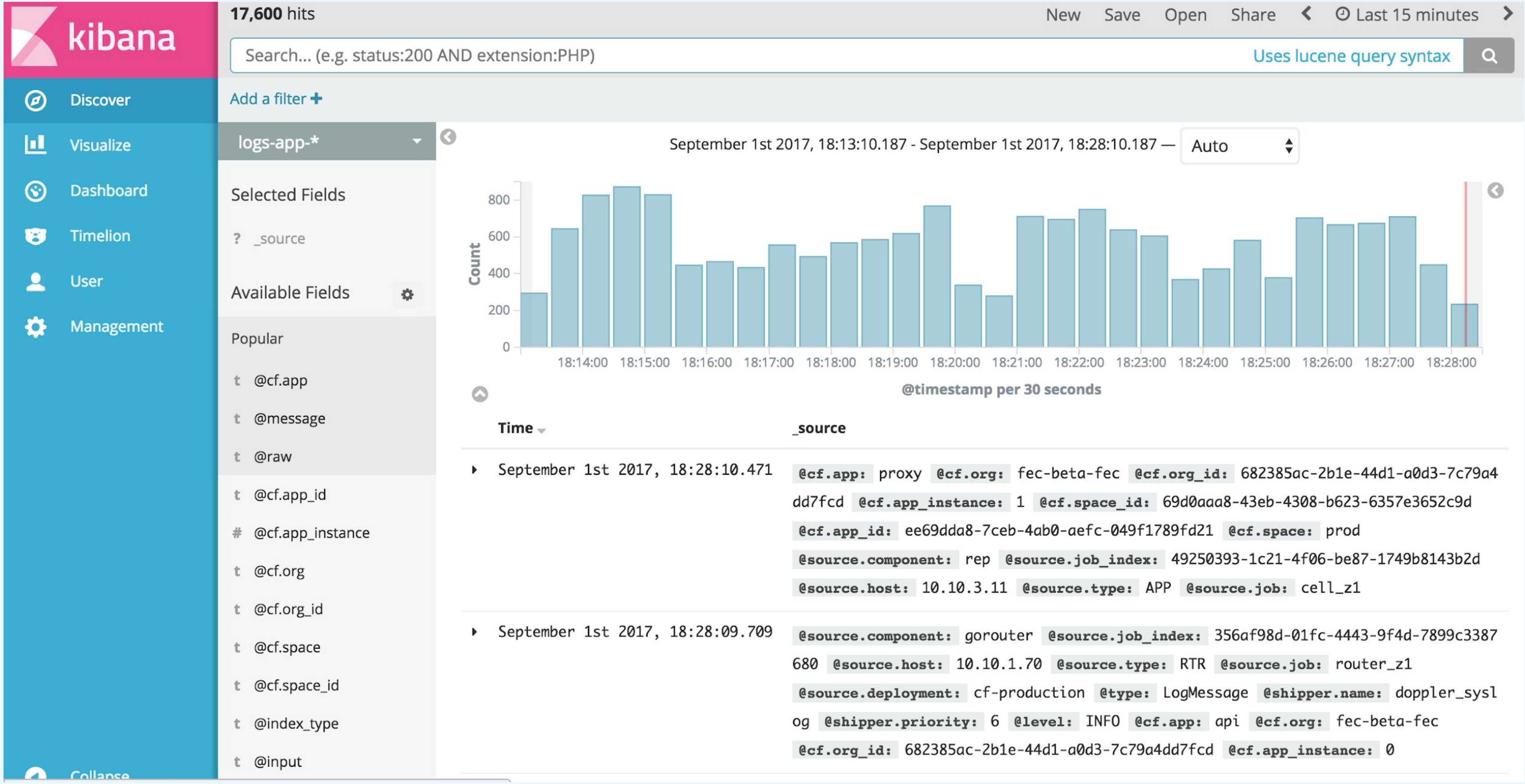
Drupal WordPress Rails Django

PostgreSQL Oracle MySQL

Built-in services

Relational databases (RDS)	PostgreSQL, MySQL, Oracle
Storage (S3)	Private or public data buckets
Custom domain	Built-in HTTPS and Content Delivery Network
Redis	In-memory data structure store
Elasticsearch	Full-text search engine
Service accounts	For continuous deployment and auditing
Identity provider	Reuse cloud.gov authentication in your apps

Built-in logging, or send logs to your own service



September 1st 2017, 18:13:10.187 - September 1st 2017, 18:28:10.187 — Auto

Time	_source
September 1st 2017, 18:28:10.471	@cf.app: proxy @cf.org: fec-beta-fec @cf.org_id: 682385ac-2b1e-44d1-a0d3-7c79a4dd7fcd @cf.app_instance: 1 @cf.space_id: 69d0aaa8-43eb-4308-b623-6357e3652c9d @cf.app_id: ee69dda8-7ceb-4ab0-aefc-049f1789fd21 @cf.space: prod @source.component: rep @source.job_index: 49250393-1c21-4f06-be87-1749b8143b2d @source.host: 10.10.3.11 @source.type: APP @source.job: cell_z1
September 1st 2017, 18:28:09.709	@source.component: gorouter @source.job_index: 356af98d-01fc-4443-9f4d-7899c3387680 @source.host: 10.10.1.70 @source.type: RTR @source.job: router_z1 @source.deployment: cf-production @type: LogMessage @shipper.name: doppler_syslog @shipper.priority: 6 @level: INFO @cf.app: api @cf.org: fec-beta-fec @cf.org_id: 682385ac-2b1e-44d1-a0d3-7c79a4dd7fcd @cf.app_instance: 0

12 factor app methodology - ideal for green-field

1 One codebase in version control, many deploys

2 Explicitly declare and isolate dependencies

3 Store config in the environment

4 Treat backing services as attached resources

5 Strictly separate build and run stages

6 Execute the app as stateless processes

7 Export services via port binding

8 Scale out via the process model

9 Maximize robustness with fast startup and graceful shutdown

10 Keep dev, staging, and prod as similar as possible

11 Treat logs as event streams

12 Run admin tasks as one-off processes

How cloud.gov reduces risk

CLOUD.GOV

GSA

18F

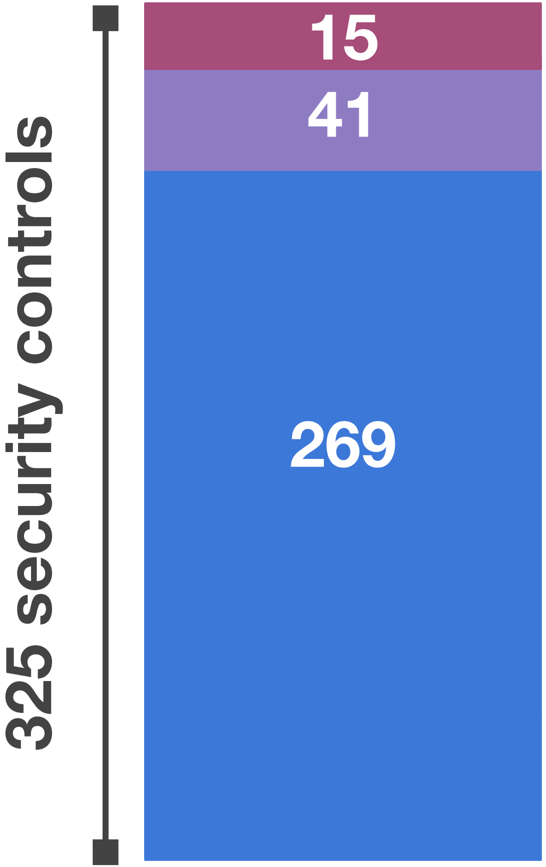
How cloud.gov reduces risk

Simplicity reduces mistakes. Plain-language configuration makes it harder to make mistakes.

cloud.gov implements the right defaults to reduce risk. Such as HTTPS and encryption at rest.

Reduce shadow IT. cloud.gov provides a modern self-service environment, so teams are less likely to use unapproved cloud infrastructure.

Many controls are handled by cloud.gov



15 customer

41 shared

269 handled or partially handled by cloud.gov
Some will be shared depending on your application

54 of these are fully inherited from AWS

How we do security

- FedRAMP Joint Authorization Board Moderate P-ATO
    - Full, verified implementation of Moderate NIST 800-53 controls
    - **Annual third-party independent audit** of controls and penetration test
    - FedRAMP Continuous Monitoring

- Secure physical infrastructure
    - AWS GovCloud US (FedRAMP JAB High P-ATO)

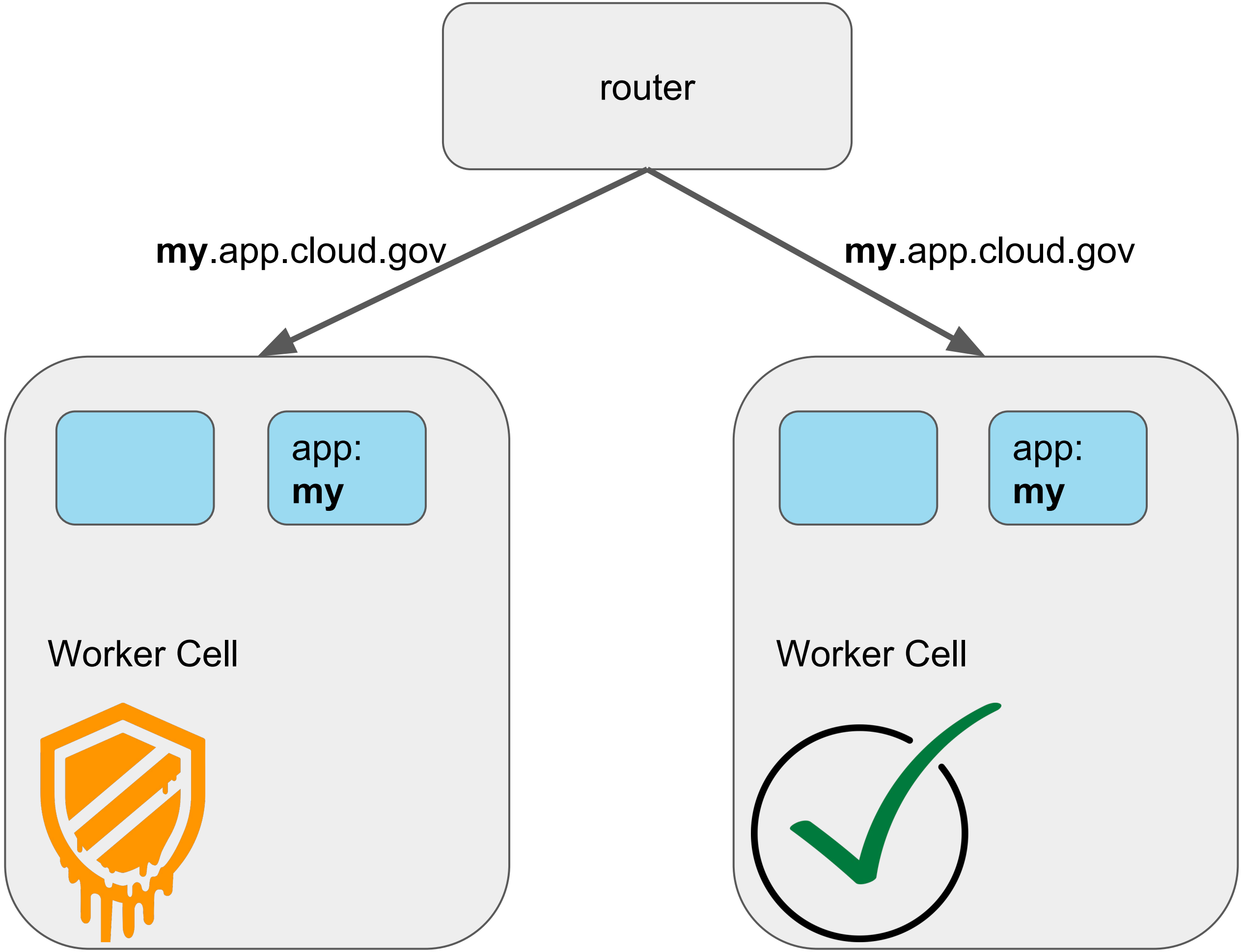
- GSA operational maturity
    - Position of Public Trust background checks

How we do security

- Architecture that isolates each customer system

- Fast, automated platform patching
  - Infrastructure as code (everything in configuration files)
  - Version control of all code and configuration
  - Continuous integration and continuous deployment
  - **Full deployment of upstream CVE patches in 12-24 hours**
  - We deploy updates several times a week

- We update without downtime or maintenance windows
  - Customer applications automatically restart, without downtime



router

my.app.cloud.gov

my.app.cloud.gov

app:
my

app:
my

Worker Cell

Worker Cell

Packages / Pricing

CLOUD.GOV

GSA 18F

Pricing

Annual access fee per system

Package	Price
Prototyping	$15,000
FISMA Low	$20,000
FISMA Moderate	$90,000

Includes:

- Basic support
- Unlimited user roles and app instances
- Development, staging, and production environments
- Most services

+

Resource use cost

Calculated based on the amount of memory (RAM) that you reserve for use by your code running in your apps.

Median is $5000 a year for current customers.

+

Services

Some services, such as especially large database instances, may incur extra costs.

CLOUD.GOV

Thank you